

Remarks

Reconsideration of this Application is respectfully requested.

Upon entry of the foregoing amendment, claims 1-44 are pending in the application, with claims 1, 21, 34, 35, and 36 being the independent claims. Claims 1-44 are sought to be amended. The changes are believed to introduce no new matter, and their entry is respectfully requested. [0091 and Fig. 4]

Based on the above amendment and the following remarks, Applicants respectfully request that the Examiner reconsider all outstanding rejections and that they be withdrawn.

Rejections under 35 U.S.C. § 102

Claim 36 was rejected under 35 U.S.C. §102(b) as allegedly being anticipated by Stallings (Cryptography and Network Security).

Claim 36 recites features that distinguish over the applied reference. For example, the claim recites access control information is stored in encrypted form in the header portion of a secure item. Thus, the access control information stays with a secure item itself, no matter where that item is located. A requestor is granted access to a secure item based on information stored in an encrypted header of the secure item.

The Stallings Kerberos server arrangement does not depend on access control information being stored as part of the secure item itself. Rather, it depends upon secret keys being shared by Kerberos servers that need to trust each other in order to extend a realm. Therefore, Stallings does not anticipate claim 36, which should be found allowable

Rejections under 35 U.S.C. § 103

Claims 1-35

Claims 1-35 were rejected under 35 U.S.C. §103(a) as being unpatentable over Samson et al. (6,339,423) in view of Boebert et al. (5,502,766).

Independent claims 1, 21, 34 and 35 recite features that distinguish over the applied references.

For example, claim 1 recites "upon successful authentication in steps (b) and (c), retrieving a user key permitting access to an encrypted header of the secured item, the encrypted header including access rules for the secured item." Claims 32, 34, and 35 recite similar features as claim 1.

The Samson et al. reference uses a token system for controlling access to a secured item. Access to resources in the domains is governed by an access control system. A first server for a first domain transmits a data token to a client seeking access to a resource in a second domain. The client transmits the data token to a second server in the other domain. The second server uses the data token to verify that the user is authentic, that is, authorized to access resources protected by the access control system. Once determining that the user is authorized to access resources, access control cookies are transmitted to client. When the client requests access to a resource in the second domain, and the request did not include access control cookies for the second domain, data is transmitted to the browser causing it to generate another request to the first server. The first server ensures that the user has been authenticated before transmitting the data token to the browser. In addition, the first server may cause copies of access control cookies for the user to be stored for later transmission to the second server. Therefore, in

contrast to the distinguishing features in the independent claims, Sampson does not appear to rely on rights/privileges stored in a secure item itself, but rather this token system.

Therefore, the applied references cannot be used to establish a prima facie case of obvious for these claims, and these claims should be found allowable.

Claims 37-42

Claims 37-42 were rejected under 35 U.S.C. §103(a) as being unpatentable over Stallings, as applied to claim 36 above, and further in view of Skarbo et al. (6,317,777).

Independent claim 36 (from which claim 37 depends) now recites access control based, at least in part, on information stored in an encrypted header of a secure item. As described above, the Stallings Kerberos server system takes a different approach as compared to the claims. Stallings Kerberos server system uses a system of secret keys exchanged between servers that must trust each other to authenticate users attached to the respective servers.

Therefore, the applied references cannot be used to establish a prima facie case of obvious for these claims, and these claims should be found allowable.

Claims 43-44

Claims 43-44 were rejected under 35 U.S.C. §103(a) as being unpatentable over Stallings and Boebert, as applied to claim 37 above, and further in view of Pensak (6,449,721 B 1).

Claim 43 also depends from and further limits claim 36, as described above. None of these references suggest storing encrypted access control information as part of the header of a secure item and the process of access control, as recited in claim 36.

Therefore, the applied references cannot be used to establish a prima facie case of obvious for these claims, and these claims should be found allowable.

Conclusion

All of the stated grounds of rejection have been properly traversed, accommodated, or rendered moot. Applicants therefore respectfully request that the Examiner reconsider all presently outstanding rejections and that they be withdrawn. Applicants believe that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

Prompt and favorable consideration of this Amendment and Reply is respectfully requested.

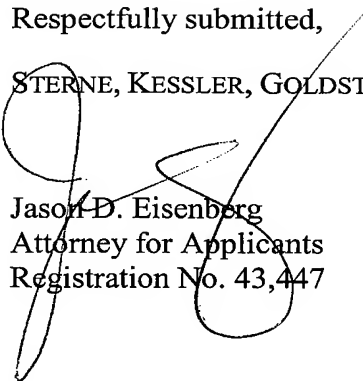
Amdt. Dated April 27, 2007
Reply to Office Action of July 14, 2006

- 21 -

VAINSTEIN *et al.*
Appl. No. 10/075,194

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.



Jason D. Eisenberg
Attorney for Applicants
Registration No. 43,447

Date: April 27, 2007

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600

670009_1.DOC